IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. JOHN CLEMENTS, Defendant.	))))))))))	CASE NO. 1:15-CR-275 JUDGE DAN AARON POLSTER **SUPPLEMENTAL MOTION TO SUPPRESS AND REQUEST FOR INDEPENDENT FORENSIC ANALYSIS OF SOFTWARE**

Now comes Defendant, John Clements, by and through undersigned counsel, Friedman & Nemecek, L.L.C., and hereby respectfully submits the instant Motion as a supplement to Defendant's Motion to Suppress, which was filed with the Court on or about March 16, 2016. (Doc. No. 22). The Defendant hereby adopts and incorporates all of the arguments and Exhibits set forth in said pleading by express reference. Counsel requests that the Court set this matter for a hearing to determine whether suppression is warranted.

Furthermore, the undersigned respectfully moves this Honorable Court to permit independent forensic analysis of the Shareaza LE software. Reasons in support of this request are set forth more fully *infra*.

Respectfully submitted,

/s/ Eric C. Nemecek
IAN N. FRIEDMAN (0068630)
ERIC C. NEMECEK (0083195)
Counsel for Defendant
Friedman & Nemecek, L.L.C.
1360 E. 9th Street, Suite 650
Cleveland, OH 44114
Phone: (216) 928-7700
Email: inf@fanlegal.com
ecn@fanlegal.com

CERTIFICATE OF SERVICE

A copy of the foregoing Motion has been served electronically this 4th day of January, 2017, to Brian McDonough, Assistant United States Attorney, United States Courthouse, Northern District of Ohio, 801 Superior Avenue W., Suite 400, Cleveland, Ohio 44113.

/s/ Eric C. Nemecek
IAN N. FRIEDMAN
ERIC C. NEMECEK
Counsel for Defendant

MEMORANDUM IN SUPPORT

I. FACTS AND PROCEDURAL HISTORY

Defendant, John Clements, is charged with one count of receiving and distributing child pornography in violation of 18 U.S.C. § 2252(a)(2)[1] and one count of possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). The Government's initial discovery response referenced a specialized computer software program, Shareaza LE, that was utilized by law enforcement agents during their investigation in this case.

After reviewing the pertinent discovery materials and conducting an independent forensic examination of Clements' electronic devices, the undersigned filed a Motion to Suppress on March 16, 2016. (Doc. No. 22). Said Motion was predicated, *inter alia*, on the contention that the Shareaza LE software enabled law enforcement to obtain information that was not available to other users of the public version of the software in violation of Clements' Fourth Amendment rights.

Upon due consideration of the information and arguments set forth in the Defendant's Motion, the Court issued an Entry dated March 17, 2016 directing the parties to have the software tested by an independent forensic expert. Thereafter, counsel for the Government suggested that Cigital perform the mandated testing. The undersigned and AUSA McDonough engaged in numerous conference calls with employees at Cigital in an effort to formulate an agreed-upon protocol for conducting the forensic examination. The Government proposed a source code analysis of both the public version of the software and the modified Shareaza LE software. Conversely, the defense indicated its desire to run

[1] Count 1 contains a date range of February 25, 2014 through May 5, 2014.

both versions of the software against a control computer so that any differences in what was obtained or reported could be documented and explained. Ultimately, the parties agreed to a multi-phase testing process whereby both the Government and defense counsel would be permitted to have the Shareaza LE software testing according to their own proposed testing protocols.[2]

On October 17, 2016, the parties appeared before the Court for a pretrial hearing to discuss the status of the software analysis that had previously been ordered. The following day, the Court issued an Order instructing the Government to have its expert provide the defense with a Report demonstrating that the use of the Shareaza LE software did not violate Clements' Fourth Amendment rights. (Doc. No. 27). The Government was required to provide said report on or before December 16, 2016. (Doc. No. 27).

After the hearing, the undersigned maintained communication with AUSA McDonough regarding efforts to try and resolve the case as well as the testing of the software. Because the Court's Order was directed at the Government, Cigital's testing focused on the code analysis that the Government had originally proposed. However, AUSA McDonough indicated his willingness to work collaboratively with counsel to procure the testing that the defense had suggested prior to the October 17th hearing.

On December 16, 2016, the undersigned received a copy of the report from Cigital regarding their analysis of the Shareaza LE software. This report is identified as Exhibit

[2] Prior to the October 17, 2016 hearing, the defense provided the Government with its proposed procedures and protocols for testing. Although the Government provided an initial draft of its proposed testing, no finalized version was ever submitted to the defense.

"A" and is incorporated herein by express reference.[3] Because the testing was exclusively code-based, counsel's expert witness, Tami Loehrs, was unable to interpret the results and/or assist counsel with respect to this issue. Accordingly, the undersigned retained Robert Kelso of Forensic Pursuit to analyze Cigital's report and provide an opinion regarding the same. Forensic Pursuit's opinion is set forth in a report dated January 3, 2017, which is identified as Exhibit "B" and incorporated herein by express reference. Because the contents of this report contain references to Cigital's report and the Shareaza LE software, the report is not attached to the instant Motion. However, the undersigned will provide a copy of the report to the Court and the Government forthwith.

II. LAW AND ARGUMENT

A. Cigital's Report Fails to Sufficiently Rebut the Alleged Fourth Amendment Violations in this Case.

Within the original Motion to Suppress, Clements' argued that the Shareaza LE software conducted a warrantless search in violation of his rights under the Fourth Amendment to the United States constitution. (Doc. No. 22). Accordingly, the Government bears the burden for establishing that no warrantless search or seizure occurred or, alternatively, that any such conduct fell within a recognized exception to the Fourth Amendment's warrant requirement.

Here, the Government is attempting to satisfy its burden through the use of Cigital's report. As previously noted, Cigital conducted a comparative analysis of the source codes for the public version of Shareaza as well as the modified version used by law enforcement

[3] Because Cigital's report contains private, proprietary information, the undersigned is not attaching a copy of the report to this Motion.

in this case (*i.e.* Shareaza LE). Cigital indicated that it found no evidence that the Shareaza LE software would have been able to access information about files that are not being intentionally shared by other Peer to Peer network users. In other words, Cigital determined that the Shareaza LE software provided the same information that would be available to anyone using the public version of the software.

Despite these conclusory statements concerning the limitations of Shareaza LE, the undersigned respectfully submits that the Government has not established that no Fourth Amendment violation occurred in this case. As the defense's expert witness explains, there are two (2) overarching flaws with Cigital's analysis that significantly undermine the Government's ability to sufficiently demonstrate that no Fourth Amendment violation occurred in this case. *See* Exhibit "B." These flaws are discussed more fully *infra*.

First, Forensic Pursuit notes that Cigital failed to provide a detailed description of all of the modifications that were made to the Shareaza LE software. In some instances, Cigital simply identified new modules that are listed by name without disclosing the programming code for the modules or describing the functionality of the modules in any significant detail. Moreover, Cigital's report does not provide any significant discussion of the database schema used by the modified code, including the specific fields being stored and example values that are typically placed into said fields. *See* Exhibit "B," p. 3-5.

For instance, Forensic Pursuit references Section 3.3.5 of Cigital's report, which is captioned "Added Files." This section of Cigital's report lists approximately twenty (20) individual program files that have been added to the publicly available version of the software. Although other portions of Cigital's report contain a description of the exact

code differences between the program files, Section 3.3.5 does not provide any discussion of the code for these approximately twenty (20) additional files. *See* Exhibit "B," p. 5. Rather, Cigital's report simply states, with no supporting evidence, that "[t]here is no security risk introduced by adding these files." *See* Exhibit "A."

Secondly, Forensic Pursuit explains that the method of analysis used by Cigital is fundamentally flawed. According to Forensic Pursuit, simply reviewing code modifications and portions of the code cannot reasonably be used by independent software analysts as a means of determining the actual functionality (*i.e.* its capabilities) of the running program. Forensic Pursuit opines that no reasonable, independent analyst can make definitive determinations or statements about what the operating program does without actually running the Shareaza LE software in a controlled test. *See* Exhibit "B," p. 4.

Forensic Pursuit explains that various factors attendant to the actual operation/use of the Shareaza LE software could alter the determination as to whether a Fourth Amendment violation occurred in this case. For instance, the use of different input data can produce dramatically different results. Such results include the possibility of exploiting weaknesses in the program that would enable the user to access files or information that are not available to other users of the program. Importantly, identifying whether any such vulnerabilities exist would be extremely difficult – if not impossible – by merely reviewing the software's code without actually running (*i.e.* testing) the software. *See* Exhibit "B," p. 5-6.

Forensic Pursuit maintains that running the Shareaza LE software in a controlled test is the only means of independently determining whether the software operates within

the purported limitations suggested by the Government or, alternatively, whether it implicates Fourth Amendment concerns. *See* Exhibit "B," p. 4. To that end, they have provided a detailed proposal for conducting the necessary testing within Section 3 of their report. *See* Exhibit "B," p. 7-10. As the report indicates, this proposed testing can be accomplished within a reasonable period of time. Likewise, any costs associated with the testing would be borne by the defense.

B. Cigital's Report Confirms that a Fourth Amendment Violation Occurred.

Within the original Motion to Suppress, Clements argued that the Shareaza LE software enabled law enforcement to obtain information that was not available to other network users who were operating the public version of the software – namely, the results of key word searches. (Doc. No. 22). The undersigned maintained that law enforcements ability to access and view such information not only violated Clements' Fourth Amendment rights, but also constituted violations of the federal Wiretap Act and/or the Stored Communications Act. (Doc. No. 22).

Although not expressly stated, Cigital's report confirms that the Shareaza LE software allowed law enforcement officers to view and record other network users' keyword search terms. *See* Exhibit "B," p. 6. Again, this information would not be accessible (*i.e.* viewable) through the publicly available version of the software. Because the particular search terms fall within the statutory definition of "content," the Government was required to obtain a warrant before such information could be obtained.

In an effort to avoid suppression, the Government has argued that the plain view exception to the warrant requirement should apply. The Government appears to suggest

that because a user's search terms are sent out over the network to other users (*i.e.* Peers) who may have the particular file(s) of interest, the communication (*i.e.* search term query) is essentially public and in plain view.

Respectfully, this logic is based on a mischaracterization or misunderstanding of how the Peer to Peer software traditionally functions. While it is true that other computers on the network will receive keyword searches entered by a particular user, that information is not accessible through the publicly available software. Rather, the recipient would not be notified that a request for files (*i.e.* search terms) had been sent to and/or processed by their computer. Furthermore, there would be no way for the recipient to access or view the particular search terms that had been submitted or the user who made the request (*i.e.* entered the search terms).

A hypothetical example will further illustrate the problematic and dangerous nature of the Government's position. Suppose that the Government exploited vulnerabilities in a common search engine – such as Google – that would allow law enforcement officers to obtain an individual's Internet search term history. Under the Government's asserted defense, this activity would be entirely permissible under the plain view doctrine despite clearly established statutory and precedent case law prohibiting such conduct in the absence of a warrant. *See* 18 U.S.C. § 2510, *et seq*; *see also In re Zynga Privacy Litigation*, 750 F.3d 1098, 1108-09 (9th Cir. 2014).

Thus, even assuming, without conceding, that Cigital's report is accurate in all other respects, the mere confirmation that Shareaza LE permits the Government to obtain content communications (*i.e.* keyword searches) submitted by other users is sufficient to justify

suppression under Fourth Amendment jurisprudence. Accordingly, the undersigned respectfully requests that this Honorable Court issue an Order suppressing and excluding any and all evidence seized that was derived from the use of the Shareaza LE software during the undercover investigation of this matter.

III. CONCLUSION

The Court's October 18th Order directed the Government to provide the undersigned with a report demonstrating that the use of the Shareaza LE software did not violate Clements' Fourth Amendment rights. (Doc. No. 27). Respectfully, Cigital's report fails to definitively establish that no Fourth Amendment violation occurred in this case. Rather, the report confirms that law enforcement was able to obtain information (*i.e.* a user's keyword searches) that is not available through the unmodified, public version of the software. Because the Government is unable to meet its burden, counsel submits that suppression of the evidence is warranted in this case.

Additionally, counsel requests that the Court permit Forensic Pursuit to conduct an independent examination of the Shareaza LE software according to the procedures and protocols set forth in Section 3 of its report. *See* Exhibit "B," p. 7-10. As aforementioned, the Government had previously indicated its willingness to collaborate with counsel's efforts to obtain independent analysis of the Shareaza LE software after Cigital's report was completed. Furthermore, the proposed testing can be accomplished within a reasonable period of time, thereby ensuring judicial efficiency. Finally, additional testing will not result in any undue burden or expense to the Government as the defense would bear the costs associated with the independent analysis.

WHEREFORE, the Defendant, John Clements, hereby respectfully requests that this Honorable Court issue an Order suppressing any and all evidence obtained by the Government – both directly and indirectly – through the use of the Shareaza LE software in the case at bar. Such request includes any evidence produced during the undercover investigation of this case as well as all evidence seized pursuant to the search warrant that was executed on June 3, 2014. Counsel further requests that the Court permit an independent forensic analysis of the Shareaza LE software according to the procedures and protocols set forth in Section 3 of Forensic Pursuit's report.

Respectfully submitted,

/s/ Eric C. Nemecek
IAN N. FRIEDMAN (0068630)
ERIC C. NEMECEK (0083195)
Counsel for Defendant
Friedman & Nemecek, L.L.C.
1360 E. 9th Street, Suite 650
Cleveland, OH 44114
Phone: (216) 928-7700
Email: inf@fanlegal.com
ecn@fanlegal.com